



ADVANCED WINDOWS

WiFi security

A WiFi network gives you a fast, reliable way of connecting PCs and printers, but for the best security you need some help from Windows. Karl Wright explains how to make your wireless network safer

If you tried wireless networking a couple of years ago and found it slow and unstable, it's time to give it another go. Wireless networking equipment is now a lot faster, running at up to 108 megabits per second (108Mbit/s). Furthermore, the equipment is much easier to set up and the range has greatly increased – just look at our wireless networking *Labs* round-up on page 157 for proof. If you want a network for your home or small office there's no reason to go for

old-fashioned wired kit. The slowest wireless connection speed is 15 to 20 times faster than a reasonably fast broadband connection.

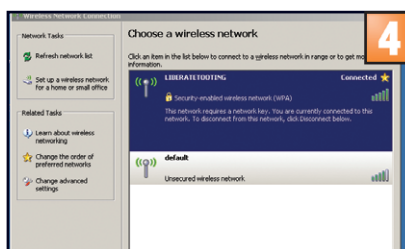
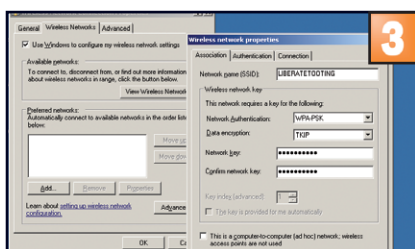
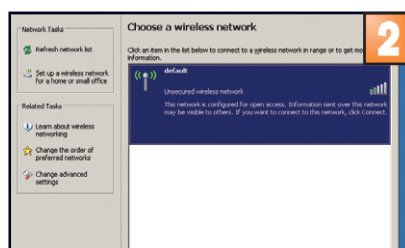
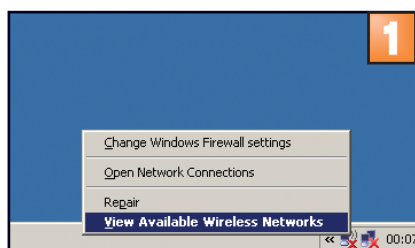
There is a catch, however: wireless networks are not secure by default. Wireless networking equipment transmits and receives data in the form of a radio signal. Anyone with a PC that's within range of this signal can tune in to it and access your network. Once they're on your network, they can attempt to break into your PCs, steal your personal

information and use your internet connection to download pornography, send spams or even hack into other people's systems.

But with a bit of know-how, you can make your wireless network so secure that even the most ingenious and determined professional hacker with plenty of time on his hands will find it hard to get past your defences. In this month's *Advanced Windows*, we'll show you how to make sure that your wireless network is safe.

HOW TO...

CONNECT A NEW PC TO YOUR NETWORK



1 Once you've hidden your network's SSID, you'll have to configure any new PCs that you want to add manually. To do this, right-click on the wireless network icon in the Windows Notification Area and choose View Available Wireless Networks.

2 A box will open, displaying the names of any networks in the area that are still openly broadcasting their SSIDs. To connect to a network you simply double-click on its name. Your network won't be listed because its name is hidden. The unsecured network you can see here belongs to a neighbour.

3 Click on Change advanced settings. Go to the Wireless Networks tab, click on Advanced and tell Windows your network's SSID and the encryption settings; see page 218. Click OK on the Advanced and Wireless Network tabs to get back to your desktop.

4 Right-click on the wireless network icon in the Windows Taskbar again but this time choose Repair. Windows will disable and re-enable your wireless network card and find the wireless network you've told it to use. As you can see, we are now connected to our network LIBERATETOOTING.

CRYPTIC PASSWORDS

First you need to create sensible passwords for every shared network resource that can be password-protected. There are a few rules to follow. Don't use something that people who know you, or know about you, will be able to guess. Don't use your child's name, your pet's name, your partner's name or any combination of their name and birthday. Don't write down your password. A good password won't be based on a name or a word you can find in the dictionary. It is a mixture of numbers and lower and upper case letters. If it has any meaning, it is only for the person who created it.

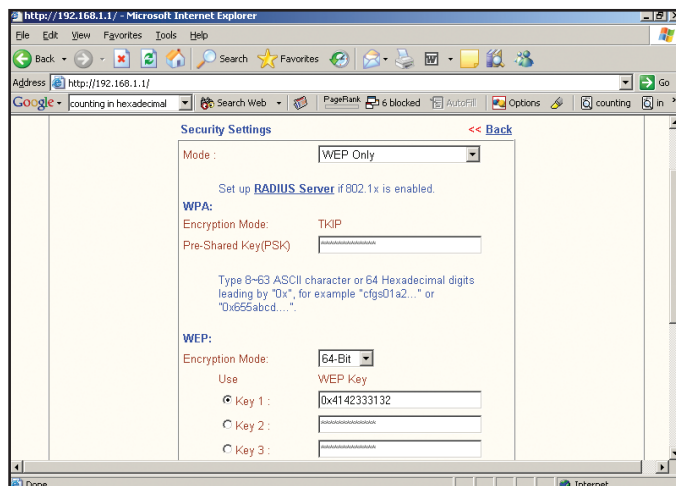
This might sound difficult, but there are ways to create a clever password you can remember. You could base your password on a phrase that you remember. For instance, your phrase might be 'I come from Glasgow. My wife is 35 years of age'. This would translate into the password lcfGMwi35y0a. As long as you don't tell anyone your phrase, this will be very difficult to guess.

To secure your wireless network, you should apply suitable passwords to your router and to the PCs on the network, assuming they're running Windows XP or another NT-based operating system. You can use these techniques when creating safe keys for wired equivalent privacy (WEP) or WiFi protected access (WPA) encryption algorithms. We'll deal with these in detail shortly.

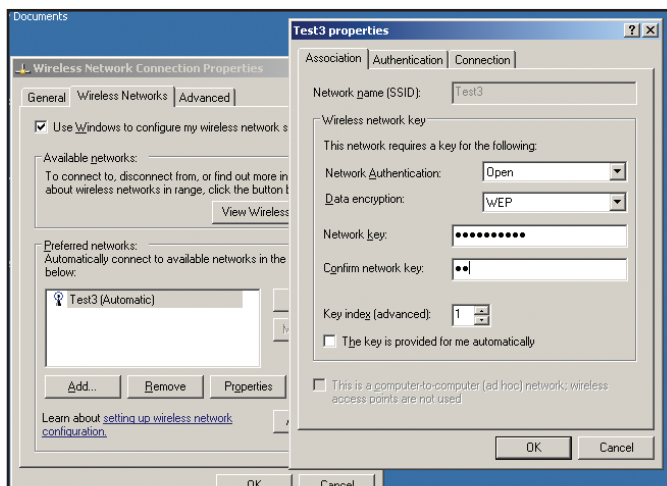
CHRISTENING YOUR NETWORK

Every wireless network has a name, known as its Service Set Identifier or SSID. Your router or access point broadcasts this name so that any PCs in range can see there's a wireless network available for them to join. When you first get your wireless network working, its name will probably be the product name of the router or the name of its manufacturer. This tells a hacker too much information about the equipment you're using, so change it immediately.

Once you've got your network set up, you can prevent your router broadcasting the SSID altogether, hiding it from anyone who doesn't already know it's there. To do this, navigate to your



Open your router's administration page in your web browser by typing the router's IP address into the browser's address bar. Navigate to the wireless security page and find the WEP configuration section, enter your WEP key and prefix if the router requires it



Open the Properties box of your wireless network and enter the WEP key you've just set up on your router. Your router may make you prefix the WEP key with other characters, but don't enter them here as Windows doesn't require it. Just enter the WEP key alone

router's HTML setup page by typing the router's Internet Protocol (IP) address into your web browser. Look for a link in the browser page called Wireless Setup or Security. On that page there should be the option to assign a new SSID and hide it. Once your network's name is hidden, connecting a new PC to the network is only a bit more complicated. Our walkthrough on the previous page shows you how it's done.

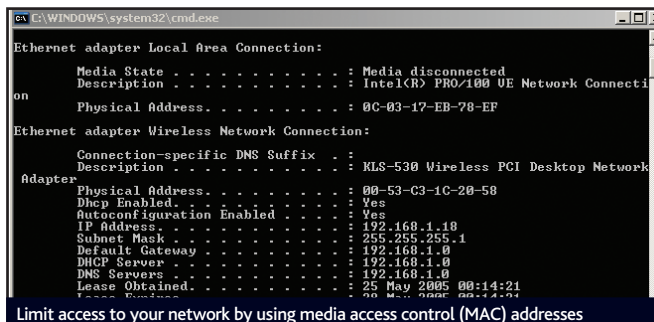
Next you need to limit access to your network by using media access control (MAC) addresses. Every network controller, wired or wireless, has a unique identifier called a MAC address. Any decent router will allow you to permit network access to computers with specified MAC addresses, and deny all others. To find out your PC's MAC address, go to Start, Run and type cmd. This brings up the command prompt. In the command box type ipconfig /all. The command prompt will display all the configuration details for each of your PC's network adaptors.

Look for your WiFi adaptor's details. These should be clearly labelled, and the adaptor's MAC address will be listed as its Physical Address. Now open your web browser and navigate to your router's control panel. Under the security settings, there will be a section called MAC Address Control or Access Control. Activate this setting and enter the MAC addresses of any PCs or other devices that you want to join the network. Any device not on your list will no longer be able to connect to your router.

ENCRYPTING YOUR NETWORK

Once you've hidden your network's SSID and limited access to specified PCs, you may think your network is secure enough. But given time and patience, even a moderately knowledgeable hacker can detect your network and fool it into giving him access by pretending to have an authorised MAC address. To make your network even more secure, you must encrypt all the data that goes across it.

Anyone who doesn't have the encryption key will be unable to access your network, even if they do manage to find it. The two main types of encryption security are WEP and WPA. We'll show you how to configure both. The following advice applies to PCs running Windows XP with Service



Limit access to your network by using media access control (MAC) addresses

Pack 2. If you don't have Service Pack 2, we strongly suggest you get it. It contains many useful security tools plus a new and improved wireless network utility. You can download it free from Microsoft and you'll also find it on the cover disc of our November issue.

WEP is the older of the two methods and is also the least secure. It contains values that, with knowledge, skill and persistence, can be discovered or derived. This makes its encryption vulnerable to attack. Unfortunately, some older WiFi equipment doesn't support the newer WPA security standard, which is more secure. Even several current, more specialised devices such as print servers and wireless video and music sharing devices don't support WPA. If you have one of these devices, WEP is the next best option.

This isn't as bad as it sounds. While WEP encryption is breakable, doing so is not easy. The chances of a hacker taking all that trouble for a home or small business network are low, particularly when there are so many other unsecured wireless networks out there.

Some routers and access points allow you to use a normal password as your WEP encryption key. The only restriction is the length of the password. If you're using 64-bit WEP encryption, you must use a five-character password. This password can contain both letters and numbers, such as AB312. If you're using the stronger 128-bit WEP encryption, you must use a 13-character password such as 1023459812DFRC. Once you've entered your password, the router automatically converts it into a hexadecimal key that can be used as the basis for encrypting your network with WEP.

Unfortunately, certain wireless devices won't let you use passwords based on normal numbers

and letters. Worse still, some routers claim to support this function, but don't. If this is the case, you will have to create your own hexadecimal number. While the decimal counting system is base 10, hexadecimal is base 16, using the numbers 0 to 9 and the letters A to F. Counting in hexadecimal looks like this: 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 1A, 1B, 1C, 1D, 1E, 1F, 20, and so on. The hexadecimal 10 corresponds to the decimal number 16; it is only after the first 15 characters have been used that hexadecimal moves into double figures.

LUCKY NUMBERS

To create a WEP hexadecimal key, you just need to know that you only use the numbers 1 to 9 and the letters A to F. A 64-bit WEP hexadecimal WEP key must be 10 digits long, so you create a 10-digit code using the numbers 0 to 9 and the letters A to F. For instance, AB134587FD is a valid key. WEP keys are case sensitive, so make sure you take a note of whether you used capital letters or not. If you want the extra security of a 128-bit WEP, your key must be 13 characters long.

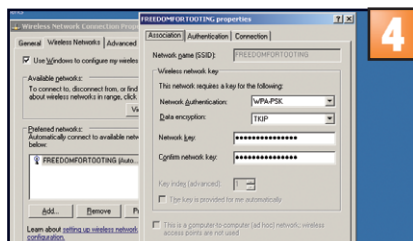
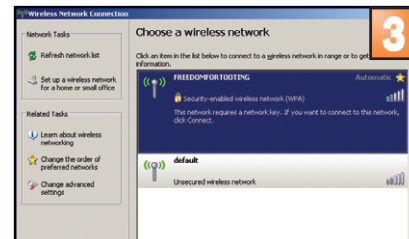
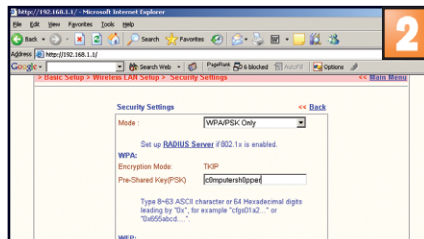
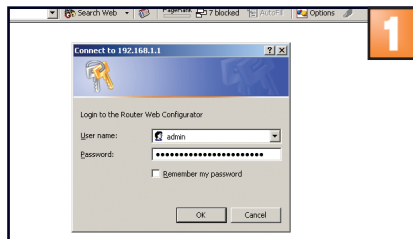
Make a note of whichever key you've chosen. Once you set your router up with WEP, you won't be able to reconnect to it wirelessly until you've configured your WiFi card to use the same key.

To set up your PC's wireless network card, right-click on the wireless network icon in the Notification Area and choose View Available Wireless Networks. Click on the entry for your wireless network and select Change advanced settings. Go to the Wireless Networks tab of the window that pops up, select your network and click on Properties. For Network Authentication choose Open; for Data Encryption choose WEP. Enter your WEP key in the boxes provided. Some routers require you to prefix the WEP key with a dollar sign or possibly the characters 0x. You don't need to enter these here; Windows won't let you so don't bother trying. Just enter the 10- or 13-character WEP key. Then press OK, return to the main wireless screen and double-click the entry for your wireless network. You should connect with no problem.

If you can't connect and the problem is with your WEP configuration then the wireless configurator will get as far as acquiring an IP



HOW TO... USE WPA ENCRYPTION



While WEP security keeps out casual snoopers and stops your neighbours from sneakily using your broadband connection for free, the newer WPA encryption standard is tougher to crack and it is also easier to set up.

1 Open your router's HTML configuration page by typing the router's IP address into your browser's address bar. Most routers have similar default IP addresses, which is why it's important that you give your router a strong password.

2 In the security section of the router's configuration page, enter your WPA password. This doesn't have to be a hexadecimal number; it can be a word or phrase

and contain numbers or any of the letters of the alphabet. Try not to be obvious; choose a password that others won't guess.

3 Once you've applied the WPA password to the router, your PC will drop its wireless network connection. To re-establish the connection, right-click on the wireless network icon in the System Tray and choose View Available Wireless Networks. Then select your network.

4 Click on Change advanced settings. Open the Wireless Networks tab, select your network and click on Properties. Go to the Association tab. Under Network Authentication, choose WPA-PSK. For Data

encryption, select TKIP. Enter your WPA password into the Network Key boxes.

5 Return to the first Wireless Network Connection box and double-click on your network. Your PC will take a few moments to connect to the network. If it hasn't connected after a minute or two, check your WPA passwords to make sure they are correct.

6 Once your PC is connected, you can surf the web and share files between computers without having to worry that someone is spying on you or using your broadband connection for free. This is very important, especially if you live in a built-up area with lots of neighbours.

address and then stop. At the end of the process, you will be connected but you won't be able to use your network. There will be a yellow triangle over the top of your Notification Area wireless network icon. If this happens, double-check that your WEP key is entered into Windows correctly. If you have another symptom, the problem probably isn't with WEP. Some routers may have problems assigning a WEP key to a network that has previously been secured using WPA. In this case, return the router to its default settings before securing it using WEP.

OTHER AUTHENTICATION METHODS

Once your network's SSID is hidden, the access is restricted to specified MAC addresses and communications are secured with either WEP or WPA (see above), this should be enough security. If you're still worried that your network could come under attack, there are other things you can do to increase your security levels.

If you don't want to use WPA with a pre-shared key (WPA-PSK), you can choose other methods of authentication instead. On the Authentication tab of your wireless network's Properties box, you will see the option to enable 802.11x. A network with 802.11x activated requires

a client PC to authenticate itself to the access point before any data – apart from the authentication packets – is transmitted. This authentication can be carried out using a username and password or a USB Smart Card with a digital certificate on it. Either way, you have the security of knowing that your user has to authenticate himself with a token, physical or notional, that is unique to him. If you're using WEP, this is a useful way of adding extra security to your network. Given the choice, though, we would use WPA-PSK.

EXTRA HELP

Depending on the capabilities of your router, there may be other security measures you can take. Some routers, for instance, allow you to set up a guest account with limited privileges. The SonicWall Soho TZW can create guest accounts that have access only to the web and cannot connect to systems on the local network. This is a convenient way of making sure that house guests or temporary workers cannot snoop around your private network.

Your router may allow you to schedule times when certain PCs are allowed to connect to the internet or your local network. If you're really worried, you could even set up a virtual private

network (VPN); see *How It Works* on page 214 for details. A VPN is an encrypted connection between two PCs, usually a client and server. It is designed to enable the transfer of files across public networks, often the internet, in complete security. Some routers can act as a VPN server. If your router does, you can configure it so anyone who wants to use the wireless network must connect to your router as a VPN server. This means your users have to remember another username and password, but it adds an extra layer of encryption to the network. For more information about VPNs, see *Advanced Windows*, *Shopper* June 2005.

SAFE FROM HARM

A wireless network is far more convenient than a wired network, and only marginally harder to set up. You don't have to drill through any walls or take cables under floorboards to share your broadband access around the house. You can sit and surf the web in front of the TV with your laptop perched on your knees.

If you follow the steps outlined here, you can be sure your wireless network's security will deter most hackers. It will certainly keep your private information safe from nosy neighbours. **CS**